



First Friday Fraud Facts+

May 6, 2016

The Office of the Idaho State Controller distributes this newsletter as a public service and as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.

Accounts Receivable Fraud

Accounts receivable fraud³ is any intentional theft or misappropriation of company revenues or assets. Most accounts receivable fraud involves diverting money before payments are recorded correctly on the company's financial records. Accounts receivable can be manipulated through a variety of schemes, for example:

- Lapping - the recording of payment(s) on a customer's account sometime after the payment has been received.
- Check kiting - overstates cash by including it in two or more bank accounts.
- Understating sales - employees skim a portion of a sale and record the transaction with a lower amount than what was actually paid.
- Substitution of check-for-cash - replacement of stolen expected payments with unexpected income, such as refunds or rebates.
- Creation of fictitious accounts and sales.

Asset misappropriations, including accounts receivable fraud, account for more than 80% of all fraud cases.

- ACFE 2014 Report to the Nations



RED FLAGS for Accounts Receivable Fraud

Here are some classic "red flags" for accounts receivable fraud³:

- Inadequate internal controls over incoming payments
- Slowing accounts receivable turnover
- Excessive write-offs of accounts receivable
- Delays in posting customer payments
- Accounts receivable detail does not agree with the General Ledger
- Customer complaints regarding statements/account balances
- Unreconciled or long-standing items on bank accounts
- Unusual employee behavior such as significant changes in spending habits, or unwillingness to take vacation

Inside This Issue:

Accounts Receivable Fraud	1
"RED FLAGS" for Accounts Receivable Fraud	1
Prevention and Detection of Accounts Receivable Fraud	2
Fraud Case : 'Grandma' Gets 33 Months for Embezzling - Woman Took \$357,200 From Highline Water District	3
Upcoming Events	4

Prevention and Detection of Accounts Receivable Fraud

According to a recent article published by the Association of Local Government Auditors, governments are susceptible to fraud areas different from the traditional for-profit entity, as net income and earning per share are not a driving factor for public entities². Combine the various fraud schemes with a small work force, or a work force with lower pay and governments find themselves struggling to provide reasonable assurance the controls in place are adequate to prevent and deter fraud. “Setting the tone at the top”, or management culture, is a critical element of preventing and detecting fraud. Management must create a culture that clearly exemplifies honesty and zero tolerance for unethical, fraudulent behavior.

Effective internal controls are the first line of defense against fraud. Improving internal control processes is one of the most effective methods for eliminating opportunity for accounts receivable fraud³.

Segregation of duties. The primary focus of segregation of duties is to separate the custodial, record keeping and supervisory/ authorization functions of the accounts receivable process. Lapping is more easily committed when one person is responsible for both the record keeping and the custody of cash³.

Increase supervision and monitoring. According to a recent study conducted by the Association of Certified Fraud Examiners, management oversight was recognized as the single most effective deterrent to fraud³. Employees who are aware of fraud detection processes will hesitate to commit fraud in fear of getting caught. Some examples of increased oversight could be: management presence at all times, video surveillance in visible locations, and ensure that employees are informed about audits that are upcoming.

Mandatory vacations and switching of job duties. This ensures that duties are rotated periodically, allowing other employees to have access to accounting records and perform the tasks that could potentially conceal accounts receivable fraud.

Validate your organizations accounts receivable. Rather than just “looking at the numbers”, pay close attention to the internal processes and controls that were used to obtain those numbers and understand what they mean. Management should take the time to question exceptions, and investigate any numbers that seem unusually high or low.



Fraud Case: 'Grandma' Gets 33 Months for Embezzling - Woman Took \$357,200 From Highline Water District

Emma Jane Martin, a 62-year-old Washington woman known to her friends and co-workers as "Grandma" began working for the public utility district in 1982 as the accounts receivable clerk.

Martin perpetrated the following fraud schemes: lapping, check-for-cash substitution and write-offs of account balances. Due to inadequate segregation of duties, Martin was in a position to both perpetrate and conceal fraud in her normal course of duties. Martin received all revenue, including checks that came in through the mail; posted customer accounts "paid"; prepared the daily bank deposit; reconciled the monthly bank account; received customer feedback, and adjusted accounts without supervisory approval.

How did she do it? Utility payments were stolen and concealed by crediting checks later received to the old account balances. Subsequent payments from other customers were applied to accounts previously manipulated, and so on. Martin also established unauthorized "suspense" accounts to conceal manipulated cash receipt transactions; she wrote-off customer account balances without proper approval; and she controlled customer feedback by placing a notice on utility bills for customers to contact her directly about problems with their accounts. No one monitored her work or composition of the daily bank deposits. There were no computer "exception" reports for account write-offs. Delinquent accounts receivables were not monitored and there were no accounts receivable aging reports to review.

How was she caught? State auditors uncovered discrepancies during a routine inspection. About that same time, district customers began finding errors on their bills and called the utility company. The state conducted a surprise audit, and Martin was fired the next day. Auditors concluded that Martin had started her fraudulent activity about 18 months prior to the state auditor findings.

Initially, district officials estimated that Martin had tampered with 800 customer accounts. By the end of the investigation that number had ballooned to over 8000. Martin plead guilty to first-degree theft and was sentenced to 33 months in prison for embezzling.

Officials at the state Auditor's Office said that it was the most ever embezzled from a water district in Washington⁴. Martin told the judge that she struggled daily to figure out what motivated her to embezzle the money.

Contact Us

Roni Harlan
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

(208) 332-8792
rhharlan@sco.idaho.gov

Visit us on the web at
www.sco.idaho.gov

Citations

¹The Fraud Triangle and What Auditors Can Do About It. <https://algaonline.org/index.aspx?NID=417>. Accessed 2 March 2016.

²Fraud Schemes: How to Prevent, Deter and Detect. <https://algaonline.org/index.aspx?NID=419>. Accessed 2 March 2016.

³How to Prevent and Detect Accounts Receivable Fraud. <http://www.zouzias.com/custom13.php>. Accessed 2 March 2016.

⁴'Grandma' Gets 33 Months For Embezzling -- Woman Took \$357,200 From Highline Water District. <http://community.seattletimes.nwsources.com/archive/?date=19980606&slug=2754700>. Accessed 28 April 2016.

Upcoming Events

11-12 May 2016 - Beginning and Intermediate Closing Package Training

For information on registering for these training opportunities, please contact us at cafr@sco.idaho.gov.